Appendix B Security Vendor Questions

This appendix contains a bank of Security Vendor Questions. This appendix contains 3 sections:

- Commercial-off-the-shelf Software
- Custom Application Set
- Hosted Application Set

Only sections that apply to the vendor solution need to be completed.

Security Vendor Questions - COTS Software Set

Commercial-off-the-shelf (COTS) software is a term for software products that are ready-made and are readily available for purchase in the commercial market

#	Question	Comments
Software History and Licensing		
1	Can the pedigree of the software be established? Briefly explain what is known of the people and processes that created the software.	
2	Explain the change management procedure that identifies the type and extent of changes conducted on the software throughout its lifecycle.	
3	Is there a clear chain of licensing from original author to latest modifier. Describe the chain of licensing.	
4	What assurances are provided that the licensed software does not infringe upon any copyright or patent? Explain	
5	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the Acquirer from these issues in the license agreement? Provide a brief explanation.	
Development Process Management		
6	What are the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software (brief summary response)?	
7	What security measurement practices and data does your company use to assist product planning?	
8	Is software assurance considered in all phases of development? Explain	
Software Security Training and Awareness		

#	Question	Comments
9	Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.	
10	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?	
11	Describe the company’s policy and process for professional certifications and ensuring certifications are valid and up-to date.	
Concept and Planning		
12	Are there some requirements for security that are “structured” as part of general releasability of a product and others that are “as needed” or “custom” for a particular release?	
13	What process is utilized by your company to prioritize security related enhancement requests?	
Architecture and Design		
14	What threat assumptions were made, if any, when designing protections for the software and information assets processed?	
15	What security design and security architecture documents are prepared as part of the SDLC process?	
16	How are design documents for completed software applications archived?	
Software Development		
17	What are/were the languages and non-developmental components used to produce the software (brief summary response)?	
18	What secure development standards and/or guidelines are provided to developers?	
19	Are tools provided to help developers verify that the software they have produced software that is minimized of weaknesses that could lead to exploitable vulnerabilities? What is the breadth of common software weaknesses covered (e.g., specific CWEs)?	

#	Question	Comments
20	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?	
Built-in Software Defenses		
21	Does the software validate (e.g., filter with white listing) inputs from untrusted sources before being used?	
22	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user) and is it designed to isolate and minimize the extent of damage possible by a successful attack?	
23	Does the documentation explain how to install, configure, and/or use it securely? Does it identify options that should not normally be used because they create security weaknesses?	
24	Where applicable, does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?	
25	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used? Are legal agreements in place to protect against potential liabilities of nonsecure software?	
Component Assembly		
26	What security criteria, if any, are considered when selecting third-party suppliers?	
27	Is the software required to conform to coding or API standards in any way? Explain.	
Testing		
28	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, integrated testing)?	
29	Who and when are security tests performed on the product? Are tests performed by an internal test team, by an independent third party, or by both?	

#	Question	Comments
30	What degree of code coverage does your testing provide?	
31	Are misuse test cases included to exercise potential abuse scenarios of the software?	
32	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?	
33	What release criteria does your company have for its products with regard to security?	
Software Manufacture and Packaging		
34	What security measures are in place for the software packaging facility?	
35	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?	
36	How is the software packaged (e.g. Zipped , Linux RPM etc) and distributed?	
37	How is the integrity of downloaded software (if an option) protected?	
38	For the released software "object", how many "files" does it consist of? How are they related?	
Installation		
39	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation? If so, how is it obtained?	
40	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?	
Assurance Claims and Evidence		

#	Question	Comments
41	How has the software been measured/assessed for its resistance to identified, relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs) used? How have the findings been mitigated?	
42	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If the CC, what evaluation assurance level (EAL) was achieved? If the product claims conformance to a protection profile, which one(s)? Are the security target and evaluation report available?	
43	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?	
44	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?	
45	Has the product undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?	
46	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)?	
Support		
47	Is there a Support Lifecycle Policy within the organization for the software in question? Does it outline and establish a consistent and predictable support timeline?	
48	How will patches and/or Service Packs be distributed to the Acquirer?	
49	What services does the help desk, support center, or (if applicable) online support system offer?	

#	Question	Comments
Software Change Management		
50	How extensively are patches and Service Packs tested before they are released?	
51	Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack automated or manual?	
52	Will configuration changes (if needed for the installation to be completed) be reset to what was there before the patch was applied in cases where the change was not made explicitly to close a vulnerability?	
53	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?	
54	Do you determine relative severity of defects and does that drive other things like how fast you fix issues?	
55	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?	
56	Are your version control and configuration management policies and procedures the same throughout your entire organization and for all your products? How are they enforced? Are third-party developers contractually required to follow these policies and procedures?	
57	What policies and processes does your company use to verify that software components do not contain unintended, “dead,” or malicious code? What tools are used?	
58	How is the software provenance verified (e.g. any checksums or signatures)?	
Timeliness of Vulnerability Mitigation		
59	Does your company have a vulnerability management and reporting policy? Is it available for review?	
60	Does your company publish a security section on its Web site? If so, do security researchers have the ability to report security issues?	

#	Question	Comments
Security "Track Record"		
61	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?	
Financial History and Status		
62	Has your company ever filed for Recompany under U.S. Code Chapter 11? If so, please provide dates for each incident and describe the outcome.	
63	Does your company have policies and procedures for periodically reviewing the financial health of the third-party entities with which it contracts for software development, maintenance, or support services?	
64	Does your company have established policies and procedures for dealing with the contractual obligations of third-party developers that go out of business?	

Security Vendor Questions- Custom Application Set

Custom software is software developed either for a specific organization or function that differs from other already available software. It is generally not targeted to the mass market but rather is usually created for specific Agencies or Business Areas.

#	Questions	Comments
Software History and Licensing		
1	Can the software pedigree be established? What is known of the people and processes that created the software (brief summary response)?	
2	Is there a change management procedure or document that will identify the type and extent of changes conducted on the software throughout its lifecycle?	
3	What assurances are provided that the software does not infringe upon any copyright or patent?	
4	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Will the supplier indemnify the Acquirer from these issues in the license agreement?	
Development Process Management		
5	What are the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software (brief summary response)?	
6	What security measurement practices and data does your company use to assist project planning?	
7	Is software assurance considered in all phases of development?	
8	How is software risk managed? Are anticipated threats identified, assessed, and prioritized?	
Software Security training and Awareness		
9	What training does your company offer related to defining security requirements, secure architecture and design, secure coding practices, and security testing?	

#	Questions	Comments
10	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?	
11	Describe the company's policy and process for professional certifications and for ensuring certifications are valid and up-to date.	
Concept and Planning		
12	Are there some requirements for security that are "structured" as part of general releasability of an application and others that are "as needed" or "custom" for a particular release?	
13	Are there some requirements for quality that are "structured" as part of general releasability of an application and others that are "as needed" or "custom" for a particular release?	
14	What review processes are implemented to ensure that nonfunctional requirements are unambiguous, traceable and testable throughout the entire SDLC?	
15	Are security requirements developed independently of the rest of the requirements engineering activities, or are they integrated into the mainstream requirements activities?	
16	Are misuse/abuse cases derived from the application requirements? Are relevant attack patterns used to identify and document potential threats?	
17	What tool(s) does your company use for requirements management?	
18	If an agile development method is used, how formally are requirements documented?	
Architecture and Design		
19	What threat modeling process, if any, is used when designing the software protections?	
20	What analysis, design, and construction tools are used by your software design teams?	
21	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to\\for review?	
Software Development		
22	What languages and non-developmental components are used to produce the software (brief summary response)?	

#	Questions	Comments
23	Does your company have formal coding standards for each language in use? If yes, how are they enforced? How often are these standards and practices reviewed and revised?	
24	Does the software development plan include security peer reviews?	
25	Are tools provided to help developers verify that the software they have produced software that is minimized of weaknesses that could lead to exploitable vulnerabilities? What is the breadth of common software weaknesses covered (e.g., specific CWEs)?	
26	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of the documentation of this methodology or provide information on how to obtain it from a publicly accessible source.	
27	Does your organization establish contractually binding agreements with their own developers and/or with their third-party developers regarding the ownership and/or licensing of intellectual property?	
28	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?	
29	Are there contractual recourses that the organization can take if a third-party developer delivers software that contains malicious code?	
30	Does the organization ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of "trigger" events.	
31	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?	

Built-in Software Defenses

#	Questions	Comments
32	Does the software validate (e.g., filter with white listing) inputs from untrusted sources before being used?	
33	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user) and is it designed to isolate and minimize the extent of damage possible by a successful attack?	
34	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?	
35	Does the exception-handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?	
36	Does the documentation explain how to install, configure, and/or use it securely? Does it identify options that should not normally be used because they create security weaknesses?	
37	Where applicable, does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?	
38	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used? Are legal agreements in place to protect against?	
Component Assembly		
39	Does the software have any security critical dependencies or need additional controls from other software (e.g., operating system, directory service, applications), firmware, or hardware? If yes, please describe.	
40	Is the software regularized to conform to coding or API standards in any way?	

#	Questions	Comments
41	Is delivery of demonstrably secure software a contractual requirement for third-party developed software? If yes, what criteria are used to operationally define “secure software”?	
42	Are additional risk management measures in place in the software’s design to mitigate risks posed by use of third-party components?	
Testing		
43	What types of functional tests are performed on the software during its development (e.g., spot checking, component-level testing, security testing, integrated testing)?	
44	Does your company’s defect classification schemes include security categories? During testing what proportion of identified defects relate to security?	
45	What degree of code coverage does your testing provide?	
46	Are misuse test cases included to exercise potential abuse scenarios of the software?	
47	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?	
48	When does security testing occur during the SDLC (e.g., unit level, subsystem, system, certification and accreditation)?	
Installation		
49	If you are responsible for installing the software, is this done by your organization or through third-party consultants?	
50	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation?	
51	What training/documentation is available for software installation and maintenance?	
Assurance Claims and Evidence		
52	Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?	

#	Questions	Comments
53	Has the software been measured/assessed for its resistance to identified relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumeration (CWEs) used? How have the findings been mitigated?	
54	Are static or dynamic software security analysis tools used to identify the weaknesses that can lead to exploitable vulnerabilities in the software? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?	
55	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?	
56	Has the software undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?	
57	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)?	
58	How is the assurance of software produced by third-party developers assessed?	
Support		
59	Are multiple tiers of support contracts available? If yes, please describe the support plans available.	
60	Is there a Support Lifecycle Policy for the software in question? Does it outline and establish a consistent and predictable support timeline?	
61	How will patches and/or Service Packs be distributed to the Acquirer?	
62	How are trouble tickets submitted? How are support issues, specifically those that security related, escalated?	

#	Questions	Comments
63	Are help desk or support center personnel internal company resources or are these services outsourced to third parties?	
64	If help desk or support center services are outsourced to third parties, are they located in foreign countries?	
Software Change management		
65	What are your policies and procedures for maintaining development documents, including requirements, design and architecture documents, source code, binaries, and user documentation?	
66	Are your version control and configuration management policies and procedures the same throughout your entire organization? How are they enforced? Are third-party developers contractually required to follow these policies and procedures?	
67	Are configuration/change controls in place to prevent unauthorized modifications or additions to source code and related documentation? Do these controls detect and report unexpected modifications/additions to source code? Do they aid in rolling back an affected artifact to a pre-modified version?	
68	Are there any undocumented features present not intended for use by end users, but available for use by the supplier for technical support and development?	
69	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?	
70	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?	
71	Does your organization have policies and procedures in place to monitor and audit the transmission of its technology-related intellectual property to third parties, and to prevent unauthorized transmission of that intellectual property?	

#	Questions	Comments
72	What policies and processes does your organization use to verify that software components do not contain unintended, “dead,” or malicious code? What tools are used?	
73	Is a process utilized by your company that can be used for documenting and analyzing the security aspects of fielded systems and for steering future improvements and modifications to those systems?	
Timeliness of Vulnerability Mitigation		
74	Does your company have a vulnerability management and reporting policy? Is it available for review?	
Individual Malicious Behavior		
75	Does your company perform background checks on members of the software development team? If so, are there any additional “vetting” checks done on people who work on critical application components, such as security? Explain.	
76	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle, along with management oversight and enforcement? Explain.	
77	What training is available to your development staff to help them identify malicious behavior? Are there formal policies for reporting malicious behavior?	
78	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.	
Organizational History		
79	Please summarize your company’s history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).	

#	Questions	Comments
80	Please provide a list of the names and dates of service of the following executive officers: • Chairman of the Board (COB) • Chief Executive Officer (CEO) • President (if different from CEO) • Vice President(s) • Chief Financial Officer (CFO)	
81	How many employees does your company have: • In the U.S.? • Worldwide?	
Foreign Interests and Influences		
82	Is the controlling share (51+%) of your company owned by a non-U.S. entity? If so, please complete Standard Form 328, Certificate Pertaining to Foreign Interests.	
83	Is your company an entity of a larger "parent" company? If yes" does that "parent" company include any subsidiaries or other sub-entities that are 51+% foreign owned? If so, please identify those subsidiaries/sub-entities.	
84	Please provide company names of all third-party entities with whom your firm contracts software development, maintenance, or support services related to this procurement.	
Financial History and Status		
85	Has your company ever filed for Recompany under U.S. Code Chapter 11? If so, please provide dates for each incident and describe the outcome.	
86	What are your company's policies and procedures for periodically reviewing the financial health of the third-party entities with which it contracts for software development, maintenance, or support services?	
87	What are your company's policies and procedures for dealing with the contractual obligations of third party developers that go out of business?	

Security Vendor Questions - Hosted Application Set

Increasingly, software is executed and maintained by someone other than the acquirer and provided as a service to them. Application service providers host the servers that support the applications in a data center and provide different levels of service, including security-related services. Users remotely access the software.

#	Questions	Comments
Service Confidentiality Policies		
1	What are your customer confidentiality policies? How are they enforced?	
2	What are your customer privacy policies? How are they enforced?	
3	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?	
4	What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same host server?	
Operating Environment for Services		
5	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?	
6	What are your policies and procedures for hardening servers?	
7	What are your data backup policies and procedures? How frequently are your backup procedures verified?	
8	What are the procedures for evaluating any vendor security alerts and installing patches and Service Packs?	
9	How are vendor patches and Services Packs applied?	
10	Is testing done after changes are made to servers? What are your rollback procedures in the event of problems resulting from installing a patch or Service Pack?	
11	What are the agents or scripts executing on servers of hosted applications? Are there procedures for reviewing the security of these scripts or agents?	

12 What are the procedures and policies used to approve, grant, monitor and revoke access to the servers? Are audit logs maintained?

13 What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?

14 Do you have a formal disaster recovery plan? What actions will be taken to recover from a disaster? Are warm or hot backups available?

15 What are the procedures used to approve, grant, monitor, and revoke file permissions for production data and executable code?

16 Is two-factor authentication used for administrative control of all security devices and critical information systems?

Security Service Available

17 What are the types of information security services you provide?

18 How are virus prevention, detection, correction, and updates handled for the products?

19 What type of firewalls (or application gateways) do you use? How are they monitored/managed?

20 What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?

21 Is your system and network architecture based on a high availability design that includes redundant firewalls, routers, switches and IDS, and load balanced or clustered servers?

Security Monitoring

22 Do you perform regular reviews of system and network logs for security issues?

23 Do you have an automated security event management system?

24 What are your procedures for intrusion detection, incident response, and incident investigation/escalation?

25 Will you provide on-site support 24x7 to resolve security incidents?

26 Do you provide write-once technology for storing audit trails and security logs?

27 How do you control physical and electronic access to the log files? Are log files consolidated to single servers?

28 Do you provide security performance measures to the customer at regular intervals?

Assurance Claims and Evidence

29 Has functional security testing been performed on the services?

30 Do you perform penetration testing of the service? If yes, how frequently are penetration tests performed? Are the tests performed by internal resources or by a third party?

31 Do you provide automated vulnerability testing of the service? If yes, how frequently are the tests performed? Are the tests performed by internal resources or by a third party?